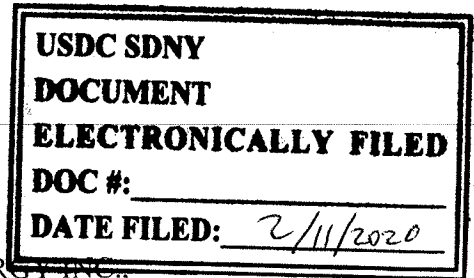


UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK



AVALON HOLDINGS CORP.

Related to:
NEW CONCEPT ENERGY INC.,

Plaintiff,
v. No. 18 CV 7291 (VSB)

Plaintiff,
v. No. 18 CIV 8896 (VSB)

GUY GENTILE and
MINTBROKER INTERNATIONAL, LTD.,

GUY GENTILE and
MINTBROKER INTERNATIONAL, LTD.,

Defendants.

Defendants.

STIPULATED PROTECTIVE ORDER WHEREAS, the Parties having agreed to the following terms governing designation, storage, use, and protection of confidential and highly confidential information and documents, and the Court having found that good cause exists for the issuance of an appropriately tailored confidentiality order ("Order") pursuant to Rule 26(c) of the Federal Rules of Civil Procedure, it is hereby

ORDERED that the following restrictions and procedures shall apply to the information and documents exchanged by the parties, as well as all information and documents provided by non-parties, including but not limited to Cboe Global Markets, Inc. ("Cboe"), in either or both of *Avalon Holdings Corp. v. Guy Gentile and Mintbroker International, Ltd.*, Case No. 18-cv-7291 (VSB) and *New Concept Energy, Inc. v. Guy Gentile and Mintbroker International, Ltd.*, Case No. 18-cv-8896 (VSB) (the "Related Cases") in connection with the pre-trial phase of the Related Cases:

1. This Order shall apply to all items or information, regardless of the medium or manner generated, stored, or maintained, including, among other things, documents, testimony, transcripts, depositions and deposition exhibits, electronically stored information ("ESI"), tangible things, and/or other information produced, given, exchanged by, or obtained by a party from any other party or any non-party during discovery in the Related Cases.
2. Counsel for any party or non-party may designate any document or information, in whole or in part, as confidential if counsel determines, in good faith, that such designation is necessary to protect the interests of the client in information that is: proprietary; a trade secret; non-public communications with regulators or other governmental bodies that are protected from disclosure by statute or regulation; information, materials, and/or other documents reflecting non-public business or financial strategies; confidential competitive information which, if disclosed, would result in competitive harm to the disclosing party; personal, client, or customer information concerning individuals or other entities, including but not limited to information that would be considered personally identifiable information under any applicable law, foreign or domestic, including but not limited to the EU

~~General Data Protection Regulation; and/or otherwise sensitive non-public information (“Confidential Information”). Information and documents designated by a party or non-party as containing, reflecting, or constituting Confidential Information will be stamped “CONFIDENTIAL.” For documents produced in native format, the producing party may include the “CONFIDENTIAL” designation in the metadata produced for such documents and on any placeholder page.~~

3. All documents and information designated as “CONFIDENTIAL” shall not be disclosed to any person, except:
 - a. The parties and their counsel, including in-house counsel;
 - b. Employees of such counsel assigned to and necessary to assist in the litigation;
 - c. Experts or consultants assisting in the prosecution or defense of the Related Cases, to the extent deemed necessary by counsel; and
 - d. The Court (including the mediator, or other person having access to any Confidential Information by virtue of his or her position with the Court, and court reporters and videographers).
4. Before disclosing or displaying the Confidential Information to any person listed in paragraphs 3(a) through 3(d) *supra*, counsel must:
 - a. Inform the person of the Confidential nature of the information or documents;
 - b. Inform the person that this Court has enjoined the use of the Confidential Information or documents by him/her for any purpose other than this litigation and has enjoined the disclosure of the Confidential Information or documents to any other person; and
 - c. Require each such person to sign an agreement to be bound by this Order in the form attached hereto (**Exhibit A**, “Agreement To Be Bound By Protective Order”).
5. “Highly Confidential Information” means information or documents that the producing party reasonably and in good faith believes contain, reflect, or constitute (i) highly sensitive information, such as current trade secrets or trading activity patterns, or other information the unauthorized disclosure of which would result in imminent competitive, commercial, or financial harm to the producing party or its personnel, clients, or customers; or (ii) material that a producing party believes in good faith would not otherwise be adequately protected under the procedures set forth herein for Confidential Information. The parties shall meet and confer before production of any document or information requiring a designation of “HIGHLY CONFIDENTIAL-ATTORNEYS’ EYES ONLY.” Any disputes regarding the

designation of “HIGHLY CONFIDENTIAL-ATTORNEYS’ EYES ONLY” that cannot be resolved by the parties’ good faith efforts to meet and confer will be resolved by judicial determination.

6. The Confidential Information (and, if applicable, any Highly Confidential Information) disclosed will be received, stored, and used by the person receiving such information in compliance with the terms of this Stipulated Protective Order and solely in connection with discovery in the Related Cases.

In the event a party challenges another party’s or a non-party’s designation of documents or information as Confidential Information, counsel shall make a good faith effort to resolve the dispute. The party challenging the designation must begin the process by notifying the designating party in writing of its challenge and identifying the challenged material with as much specificity as reasonably practical, including for example, by production number, and by providing a basis for the challenge. The challenging party and the designating party shall, within three (3) business days after service of the written objections, meet and confer concerning the challenge, unless otherwise agreed. In the absence of a resolution, the challenging party may seek resolution by the Court. Nothing in this Stipulated Protective Order constitutes an admission by any party or non-party that Confidential Information disclosed in the Related Cases is relevant or admissible. Each party reserves the right to object to the use or admissibility of any Confidential Information.

7. The disclosure of a document or information without first designating it as “CONFIDENTIAL” shall not constitute a waiver of the right to designate such document or information as Confidential Information. At the time so designated, the document or information shall thenceforth be treated as Confidential Information subject to all the terms of this Order.
8. Any party or non-party, including Cboe, may designate any portion of deposition transcripts and/or testimony as Confidential Information in writing on or before thirty (30) calendar days after the party or non-party receives the final transcript. The entire testimony shall be deemed to have been designated “CONFIDENTIAL” until the time within which the transcript or testimony may be designated has elapsed.
9. Any Personally Identifying Information (“PII”) (e.g., social security numbers, financial account numbers, passwords, and information that may be used for identity theft) exchanged in discovery shall be maintained by the receiving party in a manner that is secure and confidential.
10. Cboe is subject to, and is required to maintain the order-level data or matching engine data the parties to the Related Cases have requested (the “Cboe Data”) in conformity with Regulation SCI (“Reg. SCI”). When responding to discovery requests seeking Cboe Data, Cboe must be assured that the Cboe Data will be protected in a manner that conforms with the standards in Reg. SCI. The primary

standard identified by the SEC (“Securities and Exchange Commission”) Staff in its guidance regarding Reg. SCI compliance is the NIST 800-53 Rev. 4 framework (<https://www.sec.gov/rules/final/2014/staff-guidance-current-sci-industry-standards.pdf>). All Cboe Data shall be stored on and accessed through a system that fully complies with NIST Security and Privacy Controls for Federal Information Systems and Organizations (Special Publication 800-53 Rev. 4), available at <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>. If requested by Cboe, the parties in the Related Cases shall provide a written certification that the storage system described in the preceding paragraph has been audited for compliance with the requirements of Special Publication 800-53 Rev. 4 and fully complies therewith. For the avoidance of doubt, such Cboe Data shall not be stored on a cloud-hosted system.

11. All received ESI hosted on a review platform shall be stored in encrypted storage with access limited to those personnel actually working on this litigation and support personnel (“Credentialed Persons”). All access to such hosted systems shall be controlled in the following manner: If a Credentialed Person accesses the review platform using a computer, tablet, or cellular phone connected to the internal firm network of a law firm representing a party, then the review platform may allow such access based solely on the Credentialed Person’s law firm login information and verification that the access is through a whitelisted IP address registered to that law firm. If a Credentialed Person accesses the review platform using a computer, tablet, or cellular phone not connected to the internal firm network of a law firm representing a party, then the review platform must require the Credentialed Person to verify their identity using their regular login credentials plus a two-factor mobile device-resident authentication system that does not transmit authentication tokens through SMS text message or email (for the avoidance of doubt, systems such as RSA, Microsoft Authenticator, Google Authenticator, Duo Mobile, Symantec VIP Access, and Authy may be used for this purpose).
12. Any receiving party that shares received ESI with consultants or experts shall do so through (i) encryption in transit and shall transmit the decryption key or password to the consultants or experts, under separate cover (and not by email unless the transmission email is itself encrypted), contemporaneously with sending the encrypted media or (ii) by providing hosted access as described in the preceding paragraph.
13. In the event a receiving party’s or its expert’s or consultant’s systems are breached and any produced ESI is affected, the receiving party shall notify the party or non-party that produced the ESI within three (3) business days after becoming aware of such breach, and all affected parties and non-parties shall meet and confer immediately to address such breach. The receiving party will investigate and make reasonable efforts to remediate the effects of the breach and provide sufficient information about the breach in order to ascertain the size, scope, and nature of the breach, including but not limited to all indications of compromise relating to the breach and an analysis of whether any produced ESI related to the Related Cases was exfiltrated or altered in connection with the breach. The receiving party shall

update all other parties and non-parties that produced ESI as its breach investigation continues.

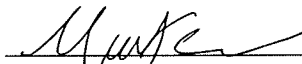
14. Pursuant to Federal Rule of Evidence 502(d), if a party or non-party, including Cboe, at any time notifies any other party that it, for any reason, disclosed documents, testimony, information, and/or things that are privileged material pursuant to attorney-client privilege, work product, the investigative privilege, including privilege over regulatory investigative techniques, procedures, means, and methods, the law enforcement privilege, or the deliberative process privilege (“Privileged Material”), or the receiving party discovers such disclosure (in which case the receiving party shall give the producing party prompt notice), the disclosure alone, pursuant to Rule 502(d), shall not be deemed a waiver – in the Related Cases or in any other proceeding, including in federal or state proceedings – of any applicable privilege or protection. In order to claw back Privileged Material that was produced inadvertently, the producing party must provide notice in writing to the receiving party or parties specifying the production number of the Privileged Material it wishes to claw back, and the basis of the claim that it is Privileged Material. Upon notice that a producing party wishes to claw back Privileged Material that was produced inadvertently, each receiving party shall promptly undertake reasonable efforts to return the Privileged Material to the producing party and destroy all summaries or copies of the Privileged Material, and shall provide to the producing party’s counsel a signed verification certifying in writing that all such Privileged Material and any copies of information or documents reflecting or constituting Privileged Material have been returned or destroyed.
15. Notwithstanding the designation of information as Confidential in discovery, there is no presumption that Confidential Information shall be filed with the Court under seal. The parties shall follow the Court’s procedures with respect to filing under seal. This Order does not govern the use of Confidential Information or Highly Confidential Information at trial; in the event either of the Related Cases goes to trial, the parties and any non-parties, including but not limited to Cboe, whose documents or information may be used at trial, shall work with the Court to develop a process to address any Confidential Information or Highly Confidential Information a party or non-party reasonably believes should not become part of the public record.
16. At the conclusion of litigation, Confidential Information (and if applicable, Highly Confidential Information) and any copies thereof shall be promptly (and in no event later than 30 days after entry of final judgment no longer subject to further appeal) returned to the producing party or certified to the producing party’s counsel as destroyed, except that the parties’ counsel shall be permitted to retain their working files on the condition that those files will remain protected.
17. If a receiving party is served with a discovery request, subpoena, or an order issued in other litigation, or receives some other form of legal process or request from any court, federal or state regulatory or administrative body or agency, legislative body,

self-regulatory organization, or other person or entity purporting to have authority to require the production thereof, that seeks disclosure of any information or items designated in the Related Cases as Confidential Information or Highly Confidential Information, the receiving party must notify, to the extent permitted by law and the rules, requirements, or requests of any relevant governmental or self-regulatory organization, the producing party (or non-party), in writing (including by electronic mail), so as to provide the producing party with a reasonable opportunity to object to the production of such materials. To the extent consistent with the rules, requirements, or requests of any relevant governmental or self-regulatory organization, the receiving party shall not produce the requested material unless and until a court of competent jurisdiction so directs, except if the producing party (a) consents, or (b) fails to file a motion to quash prior to the date designated for production of the Protected Material, in which event the receiving party may produce on the production date, but no earlier.

18. The Parties agree and stipulate that Cboe, notwithstanding its status as a non-party, shall have the right to the protections of this Stipulation and Order and to enforce the provisions contained herein.

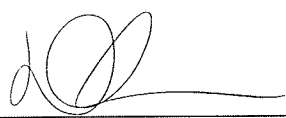
SO STIPULATED AND AGREED.

DATED: February 10, 2020
New York, NY


Miriam Tauber
MIRIAM TAUBER LAW PLLC

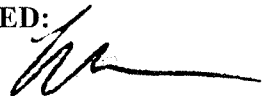
David Lopez
LAW OFFICES OF DAVID LOPEZ

*Attorneys for Plaintiffs
Avalon Holdings Corp. and
New Concept Energy, Inc.*


Adam Ford
Robert Landy
Danielle McLaughlin
FORD O'BRIEN LLP

*Attorneys for Defendants
Guy Gentile and
MintBroker International, Ltd.*

SO ORDERED:

 2/11/2020
Hon. Robert W. Lehrburger,
United States Magistrate Judge (S.D.N.Y.)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AVALON HOLDINGS CORP.		<u>Related to:</u> NEW CONCEPT ENERGY INC.,
	Plaintiff,	Plaintiff,
v.	No. 18 CV 7291 (VSB)	v. No. 18 CIV 8896 (VSB)
GUY GENTILE and MINTBROKER INTERNATIONAL, LTD.,		GUY GENTILE and MINTBROKER INTERNATIONAL, LTD.,
Defendants.		Defendants.

Exhibit A- Agreement To Be Bound By Protective Order

I have been informed by counsel that certain documents or information to be disclosed to me in connection with *Avalon Holdings Corp. v. Guy Gentile and Mintbroker International, Ltd.*, Case No. 18-cv-7291 (VSB) and *New Concept Energy, Inc. v. Guy Gentile and Mintbroker International, Ltd.*, Case No. 18-cv-8896 (VSB) (the "Related Cases") have been designated as confidential (or highly confidential, if applicable). I have been informed that any such documents or information labeled "CONFIDENTIAL" (or "HIGHLY CONFIDENTIAL-ATTORENYS' EYES ONLY," if applicable) are confidentially protected by Order of the Court.

I have been provided a copy of the Stipulated Protective Order in the Related Cases, have read its contents, and understand the obligations and restrictions therein.

I hereby agree that I will not disclose any information contained in such documents to any other person. I further agree not to store, disclose, or use any such information in violation of the Stipulated Protective Order or for any purpose other than the purpose for which counsel has directed me in this litigation.

PRINTED NAME:

Signed in the presence of:

SIGNATURE:

Name:

Attorney for:

Date:

DATE: